ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 16, Issue, 07, pp.70691-70698, July, 2026
https://doi.org/10.37118/ijdr.31033.06.2026

RESEARCH ARTICLE OPEN ACCESS

POST QUANTUM CRYPTOGRAPHY APPROACHES FOR FUTURE PROOF API SECURITY

Name Gaurav Shekhar

United States

ARTICLE INFO

Article History:

Received 19th April, 2026
Received in revised form
17th May, 2026
Accepted 20th June, 2026
Published online 30th July, 2026

Key Words:

Post-Quantum Cryptography, API Security, Quantum-Resistant Cryptography, Cryptographic Agility, Secure APIs

Corresponding author:
Name Gaurav Shekhar

ABSTRACT

Application Programming Interfaces (APIs) serve as the essential communication system which connects all contemporary digital technologies to their cloud services and mobile devices and microservices and artificial intelligence (AI) systems. APIs have decreased the time needed for digital transformation, but their use created a wider attack surface which hackers now exploit to steal data and create system failures. The security of API communications currently depends on RSA and elliptic curve cryptography (ECC) cryptographic systems which face potential dangers from fast advancements in quantum computing technology. Post quantum cryptography (PQC) has emerged as a critical response to this threat, offering cryptographic mechanisms which remain secure against both classical and quantum adversaries. This research study shows how organizations can implement PQC systems into their API security frameworks to achieve permanent protection for their data and user identity verification procedures and system security authentication methods. We evaluate how classical API security models fail to protect systems against quantum threats while we assess existing and new PQC algorithms which we test for their effectiveness in API transport security and authentication tokens and data protection. The study presents architectural patterns which support organizations to deploy hybrid and crypto agile API systems. The research team assesses performance effects through a process which compares different methods. The research results demonstrate that APIs which use PQC technology will achieve better protection against future threats but this can be done with low implementation costs if organizations include cryptographic agility and governance in their API lifecycle management systems. The study provides practical implementation pathways for industry standards which need to create a research framework to develop API ecosystems which can resist quantum attacks.

Citation: Name Gaurav Shekhar. 2026. "Post Quantum Cryptography Approaches for Future Proof API Security". *International Journal of Development Research*, 16, (07), 70691-70698.

INTRODUCTION

Application Programming Interfaces (APIs) have become essential components of contemporary digital systems because they enable different services to connect with one another across cloud platforms and mobile networks and artificial intelligence (AI) environments. APIs enable organizations to achieve modular system design and scalable system architecture and fast system development through their ability to expose data and business logic via standard interface protocols which apply to all industries from financial services to digital healthcare to autonomous systems (Behl & Behl 2024). The digital transformation process of enterprises requires APIs as essential components which act as critical connection points for user and service and device interactions.

The same characteristics which provide APIs with their ability to adapt and their ability to function exist as the system's main security vulnerabilities. The increasing use of these systems has generated a vast expansion of potential security breaches. Current research demonstrates that APIs have become the primary method for attackers to enter cloud-native systems (Salt Security, 2023). The OWASP API Security Top 10 list continues to include Broken Object Level Authorization (BOLA) and Excessive Data Exposure and Insecure Authentication as security vulnerabilities that exist within APIs (OWASP Foundation, 2023). Insufficient API governance and poor documentation and absence of runtime visibility through distributed systems create problems for these systems (Sharma & Saini, 2021). API security systems from the past depend on established security methods which use Transport Layer Security (TLS) and OAuth 2.0 for delegated authorization and

JSON Web Tokens (JWTs) as their method for managing stateless user sessions (Hardt 2012). The standards deliver three security benefits which protect against traditional security threats through their provision of data confidentiality and system integrity and user identity verification. The system protects its data through asymmetric cryptographic methods which depend on RSA and elliptic curve cryptography and discrete logarithm problem to create security through quantum computing these methods become breakable (Bernstein et al. 2020 Mosca 2021). Researchers confirmed that Shor's algorithm would allow attackers to break the algorithms within polynomial time after scalable quantum computers become operational which enables attackers to access past API sessions and create false signatures and pretend to be actual services.

The developing threat of this risk has resulted in the creation of a new security threat pattern which security experts call Harvest Now, Decrypt Later (HNDL). The attackers in this strategy begin by capturing encrypted data streams which they will store until they can use quantum technology to break the encryption (Mosca, 2021; Chen et al., 2022). The threat develops into a serious problem for APIs which process sensitive information and data that needs protection for fifty years. The data protection period of information exceeds the time which its initial cryptographic safeguards provide, therefore organizations must implement defensive measures. Post-Quantum Cryptography (PQC) provides an effective solution for current security problems. PQC describes a collection of cryptographic algorithms which researchers consider secure against both classical and quantum attacks. PQC functions entirely as a software solution which does not need quantum hardware so it can be easily implemented into current application programming interfaces (Alagic et al. 2020 NIST 2024). The NIST PQC standardization process has evaluated multiple algorithm families which include lattice-based (CRYSTALS-Kyber Dilithium) and hash-based (SPHINCS+) and code-based (Classic McEliece) algorithms (Chen et al. 2022 Campagna et al. 2022). NIST selected Kyber for key encapsulation and Dilithium for digital signatures as standardization candidates for widespread deployment in July 2022 (NIST 2024).

The process of implementing PQC for API protection requires more than just switching out existing cryptographic software. The system needs modifications to its transport protocols which include TLS 1.3 and its token-based authentication systems which use JWTs and it needs to provide cryptographic agility throughout its CI/CD processes and service mesh operations (Barker & Roginsky 2020 Bindel et al. 2021). The system must handle two performance issues which require solutions. PQC systems need bigger keys and longer signatures which create delays during handshake processes and increase data requirements for API calls that use bandwidth-sensitive operations (Al-Dabbagh et al. 2024). The organization does not yet possess sufficient preparedness for its operations. Despite recognizing the imminent threat, ISACA (2023) conducted a recent survey which discovered that only 15% of businesses started PQC risk evaluations and crypto-inventory initiatives. The knowledge deficit requires educational programs and toolchain development and policy enforcement because governments and regulators begin to create quantum-readiness standards (ENISA 2021 NSA 2022). The current security environment requires organizations to implement API protection measures through dedicated post-quantum cryptographic solutions which should be established before any advanced quantum attacks occur. Organizations should not wait until quantum computers become operational to implement their cryptographic system upgrades because this approach presents multiple operational and strategic challenges. Organizations must establish hybrid cryptographic systems which combine standard cryptography with quantum-resistant methods to protect their API processes throughout their entire operational existence from asset identification and management to their functional security and policy enforcement according to Campagna and his colleagues from 2022. Organizations can achieve post-quantum security through PQC implementation which protects their transport systems and authentication procedures and data encryption methods while creating flexible systems that support future cryptographic updates to maintain trust and data security and compliance with regulations throughout the post-quantum era.

API Security Challenges in the Quantum Era

Expanding API Attack Surface: The number of active APIs used by enterprises has increased since they started using cloud-native systems and microservices. APIs in these environments experience challenges because their development teams use multiple cloud systems and they implement continuous integration and delivery methods. Shadow APIsundocumented, outdated, or orphaned endpointspose particularly severe risks due to lack of visibility and enforcement of security controls (Salt Security, 2023). Attackers increase their targeting of APIs through direct attacks and business logic exploitation. For example, Broken Object Level Authorization (BOLA), where clients manipulate object identifiers to access data belonging to other users, remains the most commonly exploited vulnerability in real-world breaches (OWASP Foundation, 2023; Behl & Behl, 2024). The introduction of AI agents and autonomous services enables non-human actors to initiate API interactions which creates more challenges for access control and identity verification (Sharma & Saini, 2021). API security platforms face difficulties when trying to protect their systems through REST and GraphQL and gRPC and WebSocket interfaces because they encounter problems with dynamically created endpoints. The deployment frequency increases through DevOps practices but security testing fails to keep up which results in new APIs being exposed to threats from their first day of operation (Chatterjee et al., 2023).

Cryptographic Dependencies in API Security: API security architecture uses multiple layers of cryptographic mechanisms to establish secure communication while verifying identities and managing access control. TLS protects data during transmission by maintaining both confidentiality and integrity. OAuth 2.0 establishes a system that allows users to grant access through bearer tokens. The use of JWTs for stateless identity management systems has become a standard because they are normally signed with RSA or ECDSA cryptographic methods (Hardt, 2012). The security of these mechanisms relies on asymmetric cryptographic primitives that remain secure against classical attacks but become vulnerable to quantum computing advancements. Shor's algorithm enables efficient attacks against RSA and Diffie–Hellman and ECC because it operates at polynomial speed on quantum computers with sufficient processing power (Bernstein et al., 2020; Mosca, 2021). The process enables attackers to decrypt session keys which leads to data breaches while they can also forge digital signatures that undermine the trust which underpins API

security. Modern Zero Trust architectures, which are currently being used to protect API communications in distributed systems, need strong cryptographic identity management systems and secure communication channels to function effectively. The existence of quantum vulnerabilities in the cryptographic stack directly puts at risk both data security and the complete system trust boundaries (Barker & Roginsky, 2020; Chen et al., 2022).

The Quantum Threat Model: The presence of quantum adversaries creates a completely new threat framework. Quantum-capable adversaries possess unlimited access to polynomial-time solutions, which enables them to break security systems that classical attackers can only challenge through exponential-time methods. The new computational capability makes existing public-key systems unsuitable for maintaining long-term security (Campagna et al. 2022). The HNDL model presents an immediate danger because attackers currently intercept protected API communications and save them for later decoding, even though functional quantum computers have not been developed yet. The probability of this plan succeeding is particularly strong in industries that require their information to remain secret for multiple decades, which includes both healthcare and law enforcement and defense (Mosca 2021 ISACA 2023). Digital health record APIs government registry APIs and payment gateway APIs all belong to this category of high-value systems. Organizations must treat quantum resilience as an essential operational requirement instead of handling it as a mere technical challenge. Organizations need to implement safeguards that will maintain protection for their sensitive API information against current threats and future threats which will emerge after quantum computing becomes reality.

Fundamentals of Post-Quantum Cryptography: Post-Quantum Cryptography (PQC) protects against cryptographic attacks which use quantum computing power to defeat its algorithms. The software-based nature of PQC allows it to function on regular computing systems which do not require special equipment according to Bindel and his colleagues from 2021. The existing API infrastructure of cloud-native systems and mobile devices and IoT environments can use PQC because it works well with their current systems. The implementation of PQC algorithms requires more than just installation because they need proper testing to show their efficiency and safety and their implementation needs to be easy to execute. The researchers examined four key aspects which include key size and ciphertext size and signature length and computational overhead according to Al-Dabbagh et al. 2024 and Sanz et al. 2025.

PQC Algorithm Families: NIST has established its standardization procedure for post-quantum cryptographic (PQC) algorithms through its current process which classifies the algorithms into different groups based on their mathematical foundations. The most important cryptographic schemes of this group include lattice-based systems that use Kyber for key encapsulation and Dilithium for digital signature authentication. Their computational efficiency with scalable features together with their security measures make these solutions the leading options in this field. The security of lattice-based systems depends on difficult problems which include Learning With Errors (LWE) that experts believe will remain safe from attacks launched by both traditional computers and quantum machines (Alagic et al., 2020; NIST, 2024). The major category of code-based cryptography includes Classic McEliece which researchers have studied as a potential solution. It offers security through its use of error-correcting codes but its public keys become much larger than normal because its decryption process operates at high speed and the system has passed various cryptanalysis tests throughout the last thirty years (Chen et al., 2022). A third family consists of hash-based signature schemes, exemplified by SPHINCS+, which use Merkle tree structures to generate one-time and stateless digital signatures. These secure systems become impractical for applications that require fast processing because their signature sizes exceed acceptable limits in situations when users need to sign or verify their work multiple times (Bindel et al., 2021). The fourth category encompasses multivariate polynomial cryptographic systems which rely on the challenge of solving multivariate equation systems that operate in finite field environments. The lightweight applications show potential but their current state of standardization and market entrance remains behind established benchmarks. Each of these families presents distinct trade-offs regarding key sizes, signature lengths, computational cost, and implementation complexity, all of which affect their suitability for API-specific applications. Lattice-based key encapsulation mechanisms provide shorter key and ciphertext sizes than their alternative options which better serve APIs that need to achieve high throughput and low latency. Digital medical and legal documents which require permanent archival protection will accept the increased signature size that hash-based systems offer because of their strong protection capabilities (Palo Alto Networks, 2026).

NIST Standardization Effort: NIST started its international multi-stage process for evaluating and standardizing quantum-safe public-key systems in 2017 because the agency recognized the need for quantum readiness. NIST selected its first group of standardization candidates in July 2022 after conducting multiple cryptanalysis tests and performance assessments. SPHINCS+ and Classic McEliece exist as extra candidates because their security features depend on various assumption models. The selected options have been integrated into popular cryptographic software libraries which include OpenSSL and BoringSSL and wolfSSL so developers can test PQC in actual API settings. IETF is developing hybrid modes which will enable TLS and other protocols to use both traditional and quantum-resistant elements for gradual system transition according to their research efforts. The NIST project provides documentation to support cryptographic agility and migration methods for all standards which will help organizations adapt to emerging security threats and mathematical breakthroughs. The proactive standardization process guarantees future security for API systems which use PQC because they will continue to protect against evolving technological threats.

Integrating PQC into API Security Architectures: Post-quantum cryptography (PQC) presents an adaptable yet vital set of tools which organizations need to protect their APIs against future quantum computing attacks that will render conventional public-key cryptography systems obsolete. The implementation of PQC at various levels of API architecture becomes essential for protecting sensitive data which APIs transmit between remote systems because APIs function as data exchange points. The system combines multiple security features which operate at three distinct levels of defense to protect against attacks.

PQC-Enabled Transport Security: The transport layer serves as the primary and easiest integration point for PQC implementation. The modern application programming interfaces use Transport Layer Security (TLS) for their protection, which includes TLS 1.3 to secure all client-server communication. The default key exchange mechanisms in TLS which include Elliptic Curve Diffie–Hellman (ECDHE) face vulnerabilities to quantum attacks according to Campagna et al. 2022. The IETF RFC 9180 specification describes hybrid key exchange mechanisms which allow simultaneous operation of both traditional and post-quantum key encapsulation techniques. The hybrid TLS configurations maintain backward compatibility because they use two security components which protect against future breaks of their traditional elements (Paquin et al. 2020; Chen et al. 2022). The client establishes a secure session with the API gateway by starting a handshake process which uses hybrid key exchange in a typical PQC-enabled API communication system. The gateway uses post-quantum cryptographic libraries to validate the exchange process before it sends authenticated requests to backend services. This process defends session keys from future decryption attempts which protect against harvest-now-decrypt-later (HNDL) threats according to Mosca 2021.

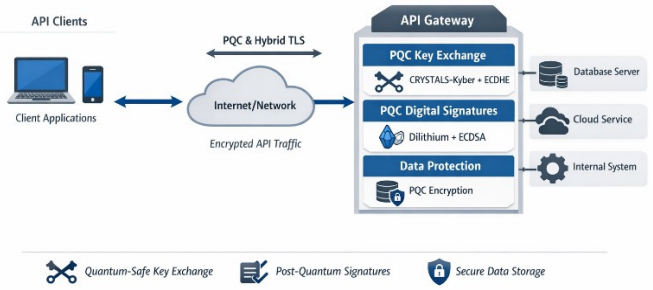

Figure 1. PQC-Enabled API Communication Architecture

The diagram shows a basic demonstration of API protection which uses PQC-based security systems that operate at the transport layer. The implementation needs both client and server systems to have matching cryptographic libraries along with API gateway and service mesh systems requiring runtime support for the deployment. The use of PQC primitives has become easier for enterprise systems because OpenSSL and wolfSSL now support more libraries for this technology (Sanz et al., 2025).

Post-Quantum Authentication for APIs: The secure authentication system for API interactions needs to verify users through JSON Web Token (JWT) authentication which uses elliptic curve digital signature (ECDSA) tokens as the core security mechanism. Quantum computers are able to solve discrete logarithm problems which creates an opportunity for attackers to forge system credentials. According to Bindel et al. 2021 and NIST 2024 CRYSTALS-Dilithium lattice-based signature technology provides post-quantum signature systems which protect against quantum-based identity theft and replay attacks. The protection of identity authentication processes in the post-quantum world benefits from PQC digital signature integration into token-based authentication systems.

Data-Centric API Protection: The application layer data protection system receives additional protection through PQC key encapsulation mechanism (KEM) keys which provide access control. This process requires the encryption of valuable API payloads which include medical records and financial data and personal identification information through the use of quantum-secure keys that come from hybrid key exchange systems. The encrypted payloads maintain their secret content even when transport layer security becomes compromised which provides an extra security layer (Al-Dabbagh et al., 2024). The implementation of PQC at this level follows zero trust principles which require all system elements and requests to undergo verification through cryptographic methods that establish their security.

Cryptographic Agility and Migration Strategies: The implementation of post-quantum cryptography (PQC) requires organizations to adopt both new cryptographic methods and significant changes to their system design and operational procedures. The implementation of PQC becomes difficult because existing systems, which include APIs, depend on their fixed security frameworks and Special cryptographic methods. Organizations need to develop a migration strategy that allows them to implement both traditional and quantum-resistant security methods. The system needs to develop cryptographic agility, which enables organizations to switch their cryptographic methods without interruption when new threats emerge or standard requirements change.

The Need for Cryptographic Agility: Future-proof API security needs cryptographic agility as its essential requirement. The system allows several cryptographic algorithm replacements or combinations without causing main application logic or data formats or network protocols to stop working. Authentication tokens which include JWTs and session negotiation routines which include TLS and storage formats which include encrypted blobs use RSA and ECDSA as their fundamental cryptographic elements in traditional deployments. The systems become unchangeable when they lack agility because cryptographic standards change through time and new vulnerabilities emerge (Barker & Roginsky, 2020). APIs require agility because they connect with external clients and third-party developers and different cloud environments. An API that uses TLS needs to provide support for a client who can only use classical cipher suites while another client needs PQC support. Flexible TLS configurations and runtime cryptographic capability negotiation and hybrid cryptographic protocol support are necessary to enable such scenarios (Paquin et al., 2020).

The requirement for organizations to adapt quickly to changing situations comes from government regulations. The NSA and NIST have developed guidelines that require organizations to create an inventory of their cryptographic assets and update those assets to safeguard against quantum threats (NSA, 2022; NIST, 2024). Organizations that manage personally identifiable information (PII) and financial data and classified information through their APIs need to establish a process that allows for quick cryptography updates to ensure they meet compliance requirements and prevent future data breaches.

Hybrid Deployment Models: Hybrid cryptographic models function as a link between established classical algorithms and newly developed PQC encryption methods. The hybrid method combines two types of algorithms which include quantum-vulnerable and quantum-safe algorithms to create multiple security layers that protect against potential threats. The hybrid TLS 1.3 key exchange system enables simultaneous operation

of ECDHE and CRYSTALS-Kyber. The first scheme (ECC) will be compromised at some point yet the second scheme (Kyber) will still protect session confidentiality according to Campagna et al. 2022. API ecosystems benefit from these models because they need to maintain backward compatibility while supporting a wide range of client systems. API consumers may range from up-to-date enterprise platforms to legacy embedded systems. Hybrid modes enable organizations to implement PQC capabilities while maintaining access for their existing clients and their older systems which need no more than endpoint updates. Hybrid cryptographic signatures provide an effective solution for systems that rely on token-based authentication. The example demonstrates that a JWT can be signed through the combination of ECDSA and Dilithium. The verifier accepts the token when at least one signature of the token validates. The model enables organizations to conduct gradual cryptographic transitions while maintaining their existing trust systems (Bindel et al., 2021). The development of migration strategies needs to include support through specialized tools. The TLS stacks of OpenSSL and BoringSSL now support hybrid modes which developers can access through their open-source libraries. The software supply chain management tools now support organizations in tracking their cryptographic dependencies through crypto-inventory scans which identify both insecure and non-agile assets (Sanz et al., 2025). Hybrid deployment functions as a strategic enabler which organizations use to advance their business objectives. It enables API-driven companies to achieve their performance and compatibility requirements while safeguarding their future security needs through the controlled implementation of PQC technology.

Performance and Overhead Analysis: The implementation of post-quantum cryptographic (PQC) systems into API security frameworks creates essential challenges which need assessment of their impact on system efficiency and processing demands and their associated practical costs. The PQC systems provide protection against future quantum threats but their resource requirements exceed those of traditional cryptographic methods because they use bigger key materials and larger signature components and they need more processing power (Al-Dabbagh et al., 2024). The usage of these systems in high-throughput settings creates operational challenges which become more significant when applied to API gateways and microservices that process thousands of requests every second. The main issue which requires attention exists because TLS handshake latency represents the initial moment when API sessions start their cryptographic negotiations. The testing results show that hybrid PQC TLS increases handshake latency by 10 to 15 milliseconds because it uses both classical elliptic curve key exchange methods and post-quantum key encapsulation mechanisms which include Kyber (Paquin et al., 2020). The system shows a substantial increase from classical TLS to current version but maintains operational limits which enterprise systems can tolerate because they need secure connections. The pure PQC modes which include Kyber-only and Dilithium-only TLS handshakes show increased latency and memory consumption because they use larger public keys and ciphertexts. The systems provide perfect protection against future decryption attacks which makes them appropriate for APIs that process confidential information which needs to be secure for extended periods or that must follow strict compliance requirements.

The table presents a summary which compares the cryptographic properties of classical and post-quantum systems.

Table 1. Comparison of Classical and PQC Cryptographic Properties

Property	RSA/ECC	Hybrid PQC	Pure PQC
Quantum Resistance	No	Yes	Yes
Key Size	Small	Medium	Large
Deployment Readiness	High	Medium	Emerging

Architectural choices for API security design emerge from these differences. Public-facing APIs which serve both legacy and modern clients will start with hybrid configurations whereas internal APIs who protect sensitive back-end services will implement pure PQC systems when they have no restrictions for latency requirements. Table 2 shows how different security modes affect average TLS handshake times to measure their impact on latency.

Table 2. API Latency Impact of PQC Integration

Security Mode	Avg. Handshake Latency (ms)
Classical TLS	35
Hybrid PQC TLS	48
Pure PQC TLS	55

The processor architecture and the cryptographic library optimization and the network bandwidth and the session resumption mechanisms create differences in the actual performance results. The optimized liboqs system which works with OpenSSL showed higher handshake throughput because the system maintained its regular API response times (Sanz et al., 2025). PQC usage results in two types of overhead through latency and increased payload size in signature-heavy APIs which require digital signatures for every response. Lattice-based schemes like Dilithium produce larger signatures compared to ECDSA, which can impact bandwidth utilization for APIs transmitting small JSON or XML payloads (Bindel et al., 2021). The size increase remains under control because the compression algorithms function as effective size reduction methods. The current system supports PQC implementation through its API stack despite existing performance limitations. Organizations can reach quantum-resilient security protections through their hybrid handshake systems by organizations implementing precise timeout threshold adjustments and caching method optimizations.

Threat Model and Security Analysis: Understanding the threat landscape is crucial for justifying the integration of PQC into API security. A comprehensive threat model must account for both classical and quantum-enabled adversaries, particularly in environments where data confidentiality is required for extended periods.

Adversary Capabilities: The post-quantum environment empowers attackers with more advanced tools than those available to standard threat operators. The adversary uses an approach which allows him to passively monitor encrypted API traffic while he collects massive amounts of information to decipher later with quantum technology according to the strategy referred to as harvest now decrypt later (Mosca 2021). The adversary can conduct both active attacks and passive surveillance experiments because he has access to quantum computers which can run Shor's algorithm, a tool that breaks

RSA and ECC encryption systems which use public-key cryptography. The system faces a security threat which impacts both its communication secrecy and data security because these algorithms protect digital signatures and key exchange processes. The advanced capabilities of adversaries allow them to conduct token forgery and replay attacks which use the collapse of cryptographic trust to impersonate real users and services within API environments. APIs in the financial sector and the healthcare industry and national security organizations face especially dangerous threats because they process sensitive and regulated data. Current cryptographic systems protect against present-day attacks but their design limits makes them unsuitable for situations that need protection against both future quantum attacks and extended security periods which need post-quantum cryptographic systems for protection.

Security Guarantees: API systems gain forward secrecy and long-term confidentiality and quantum signature protection through the integration of PQC technology. The encryption system provides protection against future decryption attempts which will remain possible until post-quantum algorithms achieve security (Chen et al., 2022; NIST, 2024). PQC-enabled digital signatures protect authorization systems by blocking adversaries from creating forged JWTs session tokens and OAuth credentials. API gateways and microservices require independent token validation because decentralized architectures need this validation for their security.

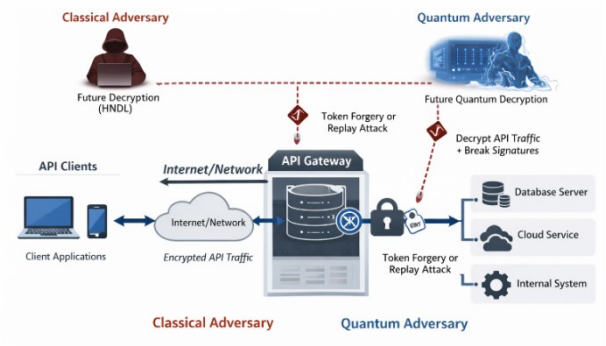

Figure 2. Threat Model for PQC-Enabled APIs

The diagram shows all the different layers of an API communication infrastructure which faces security threats from both traditional and quantum-based attackers. The system shows three main vulnerabilities which include interception points and signature forgery risks and quantum-enabled decryption scenarios.

Governance, DevSecOps, and Compliance: The process of successfully integrating PQC into API security requires both technical expertise and organizational readiness. The implementation of PQC requires organizations to establish comprehensive control mechanisms that enable them to handle ongoing software deployment while managing risks and meeting regulatory requirements. The security team must create an inventory of cryptographic operations to determine the specific contexts in which those operations occur throughout their API infrastructure. The process requires assessment of TLS configuration settings along with evaluation of JWT signing techniques and token expiration rules and third-party library components. The use of cryptographic dependency scanners enables automatic system operation, which identifies both non-agile components and elements that are vulnerable to quantum attacks (Barker & Roginsky, 2020). The DevSecOps pipelines need to implement cryptographic standards through dynamic updates after they achieve complete visibility. The system requires integration of PQC-aware linters and policy-as-code modules and runtime validators which prevent deployments that use outdated algorithms (Behl & Behl 2024). The automated testing tools need to verify handshake performance together with payload encryption and token integrity for both hybrid and PQC-only testing environments. The compliance mapping process requires alignment between cryptographic policies and NIST NSA ISO/IEC and sector-specific regulator guidance. U.S. federal agencies must implement PQC migration strategies for all national security systems according to the NSA (2022) and NIST (2024) requirements. The EU has initiated similar efforts because ENISA is establishing post-quantum readiness frameworks (ENISA 2021).

Table 3. Governance Controls for PQC-Enabled APIs

Control Area	Description
Crypto Inventory	Identification of quantum-vulnerable algorithms
CI/CD Integration	Automated enforcement of PQC policies in pipelines
Compliance Mapping	Alignment with NIST, ISO/IEC, and national regulations

Governance models need to create systems which enable APIs to adapt to changes in cryptographic technology. The system requires three components which include modular cryptographic backends and versioned token schemas and secure key rotation strategies that implement both classical and post-quantum security methods. Organizations need to create monitoring systems and auditing systems which will assess cryptographic systems and report any security breaches. Security operations must include logging and reviewing PQC handshake failure rates and token validation errors and latency thresholds as part of their standard procedures. Enterprises can achieve a secure and compliant PQC transition through governance implementation, which protects their APIs from upcoming quantum threats when they use the DevSecOps lifecycle.

DISCUSSION

The results show that post-quantum cryptography (PQC) functions as a necessary security component which organizations should use for their API security frameworks. The performance overhead from PQC algorithms creates additional system demands which include longer handshake times and larger key requirements, but these effects remain within acceptable boundaries for enterprise workloads when organizations use hybrid cryptographic systems. Organizations must evaluate their security needs against performance requirements because high-security environments need protection of sensitive information over extended periods. Organizations which adopt PQC from its start gain control over their cryptographic systems through planned execution. The system will experience urgent shifts which lead to operational outages and system conflicts and greater potential security breaches if organizations choose to delay their response until quantum threats are imminent. Through their implementation of cryptographic systems which include both quantum-resistant tests and cryptographic agility protection,

organizations can maintain their daily operations and comply with regulations while preserving customer trust during the time of cryptographic security changes.

Future Research Directions: Future research should explore the development of lightweight post-quantum cryptographic (PQC) algorithms which optimize edge APIs and Internet of Things (IoT) environments that have limited computational resources. The PQC-based API authentication schemes require formal verification methods which will confirm their accuracy and strength against adversarial attacks. The integration of PQC into AI governance frameworks provides a valuable research path which protects inference APIs while securing model integrity. Figure 3 presents a roadmap for API ecosystems to adopt PQC which shows their progression from initial assessment through hybrid deployment until they reach complete quantum-resilient operational states.

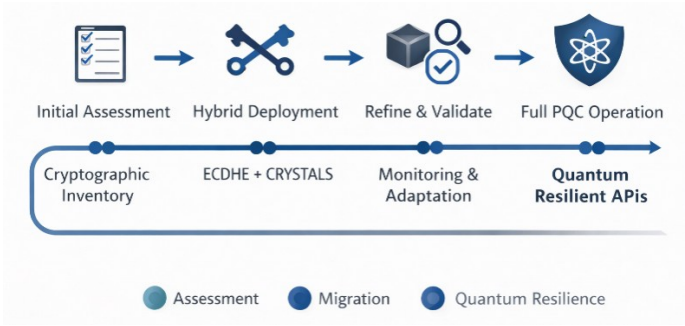

Figure 3. Roadmap for PQC Adoption in API Security

CONCLUSION

The security systems of APIs which function as the main foundation for worldwide digital systems need to undergo development because quantum computing technologies create new security threats. Standard cryptographic systems succeed in defending against traditional security threats but they now face increased risks from quantum computer-based security breaches. Post-quantum cryptography (PQC) provides a strong security solution which organizations can use to safeguard their API systems from upcoming threats. Organizations can achieve continuous protection of their API services through the implementation of PQC protection at essential system parts which include transport protocols and authentication processes and data encryption systems. The combination of PQC with cryptographic agility and automated enforcement and strong governance frameworks enables organizations to achieve compliance with regulations while maintaining operational capabilities. The systems create digital trust in an age which uses advanced intelligent systems and distributed architectures and security models which detect quantum threats to ensure that APIs will stay secure and scalable and dependable in future operations.

REFERENCES

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Yaga, D. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309

Alagic, G., et al. (2020). *Status report on the second round of the NIST post-quantum cryptography standardization process*. NIST.

Al-Dabbagh, R., Ahmad, F., & Hassan, R. (2024). Performance evaluation of post-quantum cryptographic protocols in secure API communications. *Electronics, 13*(2), 123–138. https://doi.org/10.3390/electronics13020123

Barker, E., & Roginsky, A. (2020). *Transitioning the use of cryptographic algorithms and key lengths*. NIST.

Behl, A., & Behl, K. (2024). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Bernstein, D. J., et al. (2020). Quantum-resistant cryptography. *Nature*, 549, 188–194.
https://doi.org/10.1038/s42254-019-0123-3

Bindel, N., Brendel, J., Fischlin, M., & Goncalves, B. (2021). Post-quantum security in transport protocols: Challenges and recommendations. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 312–326. https://doi.org/10.1145/3460120.3484786

Bindel, N., et al. (2021). Transitioning to post-quantum cryptography in TLS. *ACM CCS*.

Campagna, M., Celi, S., Kelsey, J., &Perlner, R. (2022). Hybrid key exchange in TLS 1.3: Analysis and implementation. *IETF RFC 9180*. https://doi.org/10.17487/RFC9180

Campagna, M., et al. (2022). Hybrid key exchange in TLS 1.3. *IETF RFC 9370*.

Chatterjee, S., Ray, I., & Krishnamoorthy, R. (2023). Securing APIs in modern microservice architectures: A comprehensive survey. *Journal of Network and Computer Applications, 210*, 103516. https://doi.org/10.1016/j.jnca.2022.103516

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2022). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

ENISA. (2021). *Post-quantum cryptography: Current state and quantum mitigation*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Hardt, D. (2012). *The OAuth 2.0 authorization framework* (IETF RFC 6749). https://doi.org/10.17487/RFC6749

ISACA. (2023). *Post-quantum cryptography: A 12-month playbook for digital trust professionals*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/post-quantum-cryptography-a-12-month-playbook

Mosca, M. (2021). Cybersecurity in an era with quantum computers. *IEEE Security & Privacy*, 19(3), 62–69.

National Institute of Standards and Technology. (2024). *NIST announces first post-quantum cryptography standards*. https://www.nist.gov/news-events/news/2024/07/nist-announces-pqc-standards

NIST. (2024). *NIST announces first post-quantum cryptography standards*. National Institute of Standards and Technology. https://www.nist.gov/news-events/news/2024/07/nist-announces-pqc-standards

NSA. (2022). *Quantum computing and post-quantum cryptography guidance for national security systems*. National Security Agency. https://www.nsa.gov

OWASP Foundation. (2023). *OWASP API security top 10*.

Palo Alto Networks. (2026). *What is post-quantum cryptography?*Cyberpedia. https://www.paloaltonetworks.com/cyberpedia/what-is-post-quantum-cryptography-pqc

Paquin, C., Stebila, D., &Tamvada, M. (2020). Benchmarking post-quantum key exchange in TLS. *ACM Workshop on Cybersecurity Experimentation and Test (CSET)*, 1–10. https://doi.org/10.1145/3408039.3408043

Salt Security. (2023). *State of API Security Report*. https://salt.security

Sanz, A., Martínez, J., Pérez, D., & Cortés, R. (2025). Comparative performance and implementation of PQC libraries in cloud environments. *arXiv preprint arXiv:2508.16078*. https://arxiv.org/abs/2508.16078

Sharma, M., & Saini, J. R. (2021). API security: Threats and defense strategies in distributed microservice environments. *Journal of Cybersecurity Technology, 5*(4), 245–268. https://doi.org/10.1080/23742917.2021.1973428

Shor, P. W. (2020). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review, 41*(2), 303–332. https://doi.org/10.1137/S0036144598347011

****